UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

Scott Boyd, on behalf of himself and all others similarly situated, Plaintiff, v. Public Employees Credit Union, Defendant.	Case No. 1:22-cv-00825 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Scott Boyd ("Plaintiff"), on behalf of himself and all others similarly situated, alleges the following Class Action Complaint (the "Action") against the above-captioned Defendant, Public Employees Credit Union (hereinafter "PECU" or "Defendant"), upon personal knowledge as to himself and his own actions, and upon information and belief, including the investigation of counsel as follows:

I. NATURE OF THE ACTION

1. Plaintiff brings this Action against Defendant for its failure to properly secure and safeguard personally identifiable information of consumers that Defendant stored on its network systems, including, without limitation, names, addresses, email addresses, telephone numbers, dates of birth, Social Security numbers, and financial information (e.g.

account numbers, credit or debit card numbers) (collectively, "personally identifiable information" or "PII").

2. PECU is an Austin, Texas based credit union offering consumers home and auto loans, insurance coverage, charge cards, checking and savings accounts, and other banking and financial services. As a requirement to access those services consumers entrust Defendant with an extensive amount of their sensitive and confidential PII.

3. On or about April 26, 2022, PECU discovered unauthorized activity on its computer network and determined that on April 24, 2022, an unknown actor accessed and obtained the PII of consumers that PECU collected and maintained as part of its regular business activities (the "Data Breach").

4. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties to those individuals, including the duty to safeguard their PII and timely notify them of unauthorized access to their PII.

5. Defendant's internal systems contain detailed and highly sensitive PII. Defendant admits that the Data Breach involved unauthorized access and activity on their internal systems and that names, or other personal identifiers in combination with Social Security numbers were affected.

6. Time is of the essence when highly sensitive PII is subject to unauthorized access and/or acquisition and it took more than two months for PECU to notify Plaintiff and Class Members of the Data Breach. The compromised PII of Plaintiff and Class Members can and likely has been sold on the dark web. Hackers access and then offer for

sale the unencrypted, unredacted PII to criminals. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing particularly sensitive information like Social Security numbers.

7. The Data Breach occurred due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiff and Class Members. It is unclear whether Defendant has yet provided notice of the Data Breach to all affected individuals, and Defendant still maintains as secret the specific vulnerabilities and root causes of the Data Breach. Plaintiff and Class Members also remain unaware of precisely what information was accessed and subject to unauthorized activity and for how long. Nearly two and a half months passed before Defendant noticed Plaintiff and Class Members that their PII was accessed and acquired by unauthorized actors leaving Plaintiff and Class Members exposed, without knowledge or recourse, for the entirety of that time.

8. This PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect PII of Plaintiff and Class Members from a foreseeable cyber-attack.

9. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of its inadequate information security practices; and (iii) comply with industry standards to protect information systems that contain PII. Defendant's conduct amounts to negligence and violates federal and state statutes. Plaintiff seeks, among other things, orders requiring Defendant to fully and

accurately disclose the nature of the information that has been compromised and to fully and accurately disclose the circumstances under which that information was compromised, to adopt reasonably sufficient security practices and safeguards to prevent future unauthorized access, disclosure, and exfiltration, and to destroy information no longer necessary to retain for purposes for which the information was first obtained from Class Members.

10. Following the breach and recognizing that Plaintiff, along with each and every Class Member, are now subject to the present and continuing risk of identity theft and fraud, Defendant offered Plaintiff and Class Members credit monitoring and identity repair services for twelve months through Experian IdentityWorks. The offered service is insufficient to protect Plaintiff and Class Members from the lifelong implications of having their most private PII accessed, acquired, exfiltrated, and/or published onto the internet. As one element of damages, Plaintiff and Class Members seek a sum of money sufficient to provide to Plaintiff and Class Members identity theft protective services for their respective lifetimes.

11. Plaintiff and Class Members have suffered injuries as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and significantly (iv) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access

and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

12. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PII was safeguarded, failing to take available steps to prevent another unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to and/or acquisition by an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

13. Plaintiff Scott Boyd is a citizen of Pflugerville, Texas, who received a Data Breach notification letter from Defendant dated July 7, 2022.

14. Defendant Public Employees Credit Union, is a Texas credit union, whose principal place of business and headquarters are at 306 East 10th St. in Austin, Texas.

15. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this

complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

16. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

17. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one other Class Member is a citizen of a state different from Defendant to establish minimal diversity under 28 U.S.C. § 1332(d)(2)(A).

18. The Western District of Texas has personal jurisdiction over Defendant named in this action because Defendant's principal place of business and headquarters are in this District and Defendant conducts substantial business in this District.

19. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant's principal place of business and headquarters are in the Austin Division of the Western District of Texas and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in Austin Texas located in the Western District of Texas.

IV. FACTUAL ALLEGATIONS

Background

20. Defendant used its internal systems to store and/or share some of Plaintiff's and Class Members most sensitive and confidential information, including but not limited

to names, addresses, email addresses, telephone numbers, dates of birth, Social Security numbers, and financial information (e.g. account numbers, credit or debit card numbers). Much of this information is static, does not change, and can be used to commit myriad financial crimes.

21. Plaintiff and Class Members relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

22. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties.

The Data Breach

23. According to Notice of Data Breach letters ("Notice Letter") Defendant sent to state Attorneys General, Defendant detected unauthorized activity on its computer network on April 26, 2022 and subsequently determined that an unauthorized person accessed and obtained certain files that contained consumer PII, including those of Plaintiff and the Class.

24. Defendant admitted in the Notice Letters that unknown party accessed and/or acquired documents that contained sensitive information about Defendant's current and former customers, including names, addresses, email addresses, telephone numbers, dates of birth, financial account information (e.g. account numbers, credit or debit card numbers), and Social Security numbers, and "other" types of personally identifiable information.

25. In response to the Data Breach, Defendant claims that it "took immediate action to contain the incident and began an investigation with the assistance of a cybersecurity firm." However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected. Learning of this information is especially important considering the sensitivity of the PII involved and the fact that it remains in Defendant's custody.

26. Plaintiff's and Class Members' unencrypted information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

27. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing their PII to be exposed.

Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' PII

28. As a condition of providing services to its customers or applicants, Defendant requires that they entrust Defendant with highly confidential PII.

29. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

30. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

31. Defendant is well aware of its obligations to protect the PII of consumers. Defendant is similarly well aware that entities like it are regularly subjected to cyber-attacks that seek to exfiltrate consumer PII for malicious purposes.

32. Defendant acknowledges the need to safeguard consumer PII on its website which states: "[s]ecurity and confidentiality are critical components of a financial institution's online banking system." PECU further reassures consumers that it, "…understands the security and privacy issues and concerns involved in an online banking environment." And that it is, "…committed to provide safe and secure measures to protect PECU members account information and financial transactions…"[1] Unfortunately for Plaintiff and Members of the Class, Defendant failed to keep their PII secure and confidential as it knew it should.

Securing PII and Preventing Breaches

33. Defendant could have prevented this Data Breach by properly securing and encrypting the PII of Plaintiff and Class Members. Defendant could have also destroyed data that it no longer required, especially data from former customers or applicants.

[1] https://www.pecutx.org/services/e-branch-security/

34. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to it about protecting and securing sensitive data.

35. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is further exacerbated by its own knowledge of the likelihood of a data breach, the need to guard against such attacks, and the consequences to Plaintiff and the Class resulting from a successful data breach.

36. Defendant's own website recognizes the need to protect PII and that entities like it are a regular target of cyber-attacks:

> …recent social engineering attacks against two-factor authentication demonstrate that you can't rely on technology alone. We have become aware of several incidents at other institutions in which criminals have tried to bypass the protection offered by two-factor authentication. The attacks employ phishing messages, fake login pages, and persuasive follow-up to induce the victim to give up an authentication code.[2]

37. Despite Defendant's awareness of previous data breaches targeting financial institutions and the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

38. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,"

[2] https://www.pecutx.org/services/fraud-center/

including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

39. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of PII

40. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200. Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web. Criminals can also purchase access to entire company data breaches from $900 to $4,500.

41. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for

> credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.

42. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

43. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."

44. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—name, Social Security number, and potentially date of birth.

45. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."

46. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

47. The PII of Plaintiff and Class Members was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

48. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

49. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if the PII was compromised, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members a result.

50. Plaintiff and Class Members are each now subject to the present and continuing risk of identity theft and fraud and now face years of constant surveillance of

their financial and personal records, monitoring, and loss of rights. Plaintiff and Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

51. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on its file servers which contained detailed, personal information on thousands of consumers and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

52. Following the breach and recognizing that Plaintiff, along with each and every Class Member, is now subject to the present and continuing risk of identity theft and fraud, Defendant offered Plaintiff and Class Members twelve months of identity monitoring services. The offered service is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

53. Moreover, Defendant put the burden squarely on Plaintiff and Class Members to enroll in the inadequate monitoring services, among other steps Plaintiff and Class Members must take to protect themselves. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.

54. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week; leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'" Usually, this time can be spent at the option and choice

of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves. Defendant states its affected current and former customers to "should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis."

55. Plaintiff and Class Members are now deprived of the choice as to how to spend their valuable free hours and seeks remuneration for the loss of valuable time as another element of damages.

56. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Defendant Violated the Gramm-Leach-Bliley Act

57. Defendant is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3)(A), and thus is subject to the GLBA.

58. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

59. Defendant collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Defendant was subject to the requirements of the GLBA, 15 U.S.C.

§§ 6801.1, *et seq*., and is subject to numerous rules and regulations promulgated on the GLBA statutes.

60. The GLBA Privacy Rule became effective on July 1, 2001. See 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

61. Accordingly, Defendant's conduct is governed by the Privacy Rule prior to December 30, 2011 and by Regulation P after that date.

62. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous." 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These

privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Defendant violated the Privacy Rule and Regulation P.

63. Defendant failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing that PII on Defendant's network systems.

64. Defendant failed to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers' PII on an insecure platform, accessible to unauthorized parties from the internet, and would do so after the customer relationship ended.

65. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer

information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4. As alleged herein, Defendant violated the Safeguard Rule.

66. Defendant failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information.

67. Defendant failed to adequately evaluate and adjust its information security program in light of the previous data breach, changes to its business operation, and other relevant circumstances, including the heightened cyber-attack risk environment.

68. Defendant violated the GLBA and its own policies and procedures by sharing the PII of Plaintiff and Class Members with a non-affiliated third party without providing Plaintiff and Class Members (a) an opt-out notice and (b) a reasonable opportunity to opt out of such disclosure.

Plaintiff's Experience

69. In or about 2016, Plaintiff Boyd used PECU's services to acquire an auto loan. In connection with his loan application, Mr. Boyd was required to provide highly sensitive information to Defendant, including his Social Security number and financial information.

70. On or about July 7, 2022, Plaintiff Boyd learned of the Data Breach via a notice from Defendant that informed Plaintiff Boyd that his name, financial information, and Social Security number had been compromised. Plaintiff Boyd was surprised that his PII had been acquired by a cyber-attacker in the Data Breach because he had long since

paid off his loan and did not believe there was any reason for PECU to continue to maintain his PII.

71. Plaintiff is particularly concerned about the fact that his Social Security number was obtained by a cyber-attacker because he is an employee of the federal government and the misuse of his PII or the theft of his identity could result in his being unable to perform his regular work activities.

72. After learning of the Data Breach, Plaintiff Boyd spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Data Breach, researching identity theft protection services, signing up for the identity monitoring service detailed in the Notice Letter, self-monitoring his financial accounts, and monitoring all services on a regular basis. This time has been lost forever and cannot be recaptured.

73. Plaintiff has also noticed an increase in the number of spam emails he receives that began following the Data Breach. Plaintiff believes these to be related to the Data Breach due to the timing and as the emails are often solicitations for banking services, like those offered by Defendant.

74. Additionally, Plaintiff Boyd is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. Plaintiff Boyd stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

75. Plaintiff Boyd suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Plaintiff Boyd entrusted to Defendant as a customer, which was compromised in and as a result of the Data Breach.

76. Plaintiff Boyd suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy. This is compounded by the fact that Plaintiff is a federal government employee and any misuse of his PII would cause significant interference with his ability to perform his work.

77. Plaintiff Boyd has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, in combination with his name being placed in the hands of unauthorized third-parties and possibly criminals.

78. Plaintiff Boyd has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

79. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

80. The Class that Plaintiff seeks to represent is defined as follows:

> All individuals residing in the United States whose PII was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Public Employees Credit Union on or about July 7, 2022 (the "Nationwide Class").

81. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members and staff.

82. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

83. **Numerosity, Fed R. Civ. P. 23(a)(1):** The Nationwide Class (the "Class") is so numerous that joinder of all members is impracticable. Defendant reported to the Attorney General of Indiana that more than 28,000 individuals were affected by the Data Breach.[3]

84. **Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3):** Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

[3] *See* https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/files/Data-Breach-year-to-date-Report.pdf at line 554.

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant had a duty not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had a duty not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

e. When Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual, damages, and/or statutory damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

85. **Typicality, Fed. R. Civ. P. 23(a)(3):** Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

86. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

87. **Adequacy, Fed. R. Civ. P. 23(a)(4):** Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class

Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intend to prosecute this action vigorously.

88. **Superiority and Manageability, Fed. R. Civ. P. 23(b)(3):** The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

89. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and

individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

90. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

91. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

92. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to act unlawfully as set forth in this Complaint.

93. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

94. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members; and,

i. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE

95. Plaintiff fully re-alleges the aforementioned paragraphs and the below paragraphs as if fully enumerated herein.

96. Plaintiff brings this cause of action on his own behalf and that of the Class.

97. As a condition of being customers of Defendant, Defendant's current and former customers were obligated to provide and entrust Defendant with certain PII, including their names, addresses, email addresses, telephone numbers, dates of birth, financial account numbers, and Social Security numbers.

98. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

99. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

100. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

101. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiff and the Class in Defendant's possession was adequately secured and protected.

102. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customers' PII it was no longer required to retain pursuant to regulations.

103. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and the Class.

104. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of being customers of Defendant.

105. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

106. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

107. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

108. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII of Plaintiff and the Nationwide Class, including basic encryption

techniques freely available to Defendant and failing to delete PII it no longer had a reasonable business need to maintain.

109. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

110. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

111. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

112. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Class.

113. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

114. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Class during the time the PII was within Defendant's possession or control.

115. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

116. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiff and the Class in the face of increased risk of theft.

117. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of its current and former customers' PII.

118. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove former customers' PII it was no longer required to retain pursuant to regulations.

119. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

120. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the PII of Plaintiff and the Class would not have been compromised.

121. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

122. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or

practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

123. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

124. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

125. Defendant's duty to use reasonable security measures also arose under the GLBA, under which Defendant was required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

126. Defendant violated the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule by (a) failing to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing and/or sharing that PII on Defendant's internal systems that were inadequately secured and accessible to unauthorized third-parties from the internet, (b) failing to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers' PII on such an insecure platform and/or system, (c) failing to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information, (d) failed to

adequately (i) test and/or monitor the system where the Data Breach occurred and (ii) update and/or further secure its data security practices in light of the heightened risk environment.

127. Defendant's violation of the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule constitutes negligence.

128. Plaintiff and the Class are within the class of persons that the FTC Act and the GLBA were intended to protect.

129. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class. The GLBA, with its Privacy Rule, Regulation P, and Safeguards Rule, was similarly intended to guard against harms such as the harm that occurred as a result of the Data Breach.

130. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent,

detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

131. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

132. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT

133. Plaintiff fully re-alleges the aforementioned paragraphs and the below paragraphs as if fully enumerated herein.

134. Defendant required Plaintiff and the Class to provide their personal information, including names, Social Security numbers financial information, and other personal information, as a condition of being customers of Defendant.

135. As a condition of being customers of Defendant, Plaintiff and the Class provided their personal and financial information. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

136. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

137. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal and financial information, including by failing to implement basic encryption techniques freely available to Defendant and failing to delete PII it no longer had a reasonable business need to maintain, and by failing to provide timely and accurate notice to them that personal and financial information was compromised as a result of the data breach.

138. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential

data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

THIRD CAUSE OF ACTION
INVASION OF PRIVACY

139. Plaintiff fully re-alleges the aforementioned paragraphs and the below paragraphs as if fully enumerated herein.

140. Plaintiff and the Class had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

141. Defendant owed a duty to its current and former customers, including Plaintiff and the Class, to keep their PII contained as a part thereof, confidential.

142. Defendant failed to protect and released to unknown and unauthorized third parties the PII of Plaintiff and the Class.

143. Defendant allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiff and the Class, by way of Defendant's failure to protect the PII.

144. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and the Class is highly offensive to a reasonable person.

145. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and the Class is of no legitimate concern to the public.

146. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Class disclosed their PII to Defendant as part of the current and former customers' relationship with Defendant, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

147. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

148. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

149. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Class.

150. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiff and the Class was disclosed to third parties without authorization, causing Plaintiff and the Class to suffer damages.

151. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

152. As a direct and proximate result of Defendant's invasion of privacy, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

FOURTH CAUSE OF ACTION
BREACH OF CONFIDENCE

153. Plaintiff fully re-alleges the aforementioned paragraphs and the below paragraphs as if fully enumerated herein.

154. At all times during Plaintiff's and the Class's interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and the Class Members' PII that Plaintiff and the Class provided to Defendant.

155. As alleged herein and above, Defendant's relationship with Plaintiff and the Class was governed by terms and expectations that Plaintiff's and the Class Members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

156. Plaintiff and the Class provided their PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized third parties.

157. Plaintiff and the Class also provided their PII to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PII from unauthorized disclosure.

158. Defendant voluntarily received in confidence the PII of Plaintiff and the Class with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

159. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, the PII of Plaintiff and the Class was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and the Class Members' confidence, and without their express permission.

160. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and the Class have suffered damages.

161. But for Defendant's disclosure of Plaintiff's and the Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. The Data Breach was the direct and legal cause of the theft of Plaintiff's and the Class Members' PII as well as the resulting damages.

162. The injury and harm Plaintiff and the Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and the Class Members' PII. Defendant knew or should have known its methods of accepting and securing PII was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and the Class Members' PII.

163. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Class, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of current and former customers; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

164. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

VII. PRAYER FOR RELIEF

165. WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class and appointing Plaintiff and his Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

   a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

   b. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

   c. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the

retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

d. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

e. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

f. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

g. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

h. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

i. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

j. requiring Defendant to conduct regular database scanning and securing checks;

k. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

l. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

m. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

n. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

o. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

p. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, statutory, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

VIII. JURY TRIAL DEMAND

Plaintiff hereby demands that this trial be tried before a jury.

Dated: August 12, 2022

Respectfully submitted,

/s/ Joe Kendall

JOE KENDALL
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 1450
Dallas, Texas 75219
214-744-3000 / 214-744-3015 (Facsimile)
jkendall@kendalllawgroup.com

Gary M. Klinger
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866-252-0878
Email: gklinger@milberg.com